PCT / SE 2004 / 000945

PA 1191787

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

July 08, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: ***60/479,156***
FILING DATE: ***June 18, 2003***

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

T. WALLACE
Certifying Officer

16179 U.S. PTO
06/18/03

60479156 06/18/03

Mail Stop Provisional Patent Application

PTO/SB/16 (6-95)
Approved for use through 04/11/98. OMB 0651-003
Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

PROVISIONAL APPLICATION COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION under 37 CFR 1.53 (c).

	Docket Number	4147-36	Type a plus sign (+) inside this box→	+

INVENTOR(S)/APPLICANT(S)

LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)
OYAMA	Johnson		Tokyo, Japan
KATO	Ryoji		Yokosuka Kanagawa, Japan

16235 U.S. PTO 60/479156

TITLE OF THE INVENTION (280 characters)

AUTHENTICATION METHOD

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☒ **Customer Number:** 23117

Type Customer Number here

Place Customer Number Bar Label Here →

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒	Specification	Number of Pages	14	☐	Applicant claims "small entity" status. ☐ "Small entity" statement attached.
☒	Drawing(s)	Number of Sheets	4	☐	Other (specify)

METHOD OF PAYMENT *(check one)*

☒	A check or money order is enclosed to cover the Provisional filing fees ($160.00)/($80.00)	PROVISIONAL FILING FEE AMOUNT ($) 160.00
☒	The commissioner is hereby authorized to charge filing fees and credit Deposit Account Number 14-1140	

The invention was made by an agency of the United States Government or under a contact with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE _____ Reg No. 27,393 DATE June 18, 2003

TYPED or PRINTED NAME H. Warren Burnam, Jr. REGISTRATION NO. *(if appropriate)* 29,366

☐ Additional inventors are being named on separately numbered sheets attached hereto.

PROVISIONAL APPLICATION FILING ONLY

Burden Hour Statement: This form is estimated to take .2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Mail Stop Comments - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, and to the Office of Information and Regulatory Affairs, Office of Management and Budget (Project 0651-0037), Washington, DC 20503. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Mail Stop Provisional Patent Application**, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

749107

Our Ref.: 4147-36
PE18387US00

U.S. PROVISIONAL PATENT APPLICATION

Inventor(s): Johnson OYAMA
Ryoji KATO

Invention: AUTHENTICATION METHOD

NIXON & VANDERHYE P.C.
ATTORNEYS AT LAW
1100 NORTH GLEBE ROAD, 8TH FLOOR
ARLINGTON, VIRGINIA 22201-4714
(703) 816-4000
Facsimile (703) 816-4100

SPECIFICATION

749109

[redacted]

AUTHENTICATION METHOD

TECHNICAL FIELD

The present invention generally relates to communication networks comprising mobile nodes and in particular to Mobile Internet Protocol (MIP) authentication.

BACKGROUND

Mobile IPv6 (MIPv6) capable mobile nodes, such as cellular phones, laptops and other end-user equipment, can roam between networks that belong to their home service provider as well as others. Roaming in foreign networks is enabled as a result of the service level and roaming agreements that exist between operators. One of the key AAA protocols that contribute to making this kind of a roaming mechanism possible is Diameter and the general architecture for MIPv6 AAA is schematically illustrated in Fig. 1.

Finding a well-functioning and complete MIPv6 AAA solution combining mobility with authentication/security for mobile communication would be very desirable. For instance, AAA can then be used to check/control who is entering the network. However, in the prior art only partial solutions are presented. These are generally non-consistent with each other and do not work end to end.

In [4], for example, attempts are made to specify a new application to Diameter enabling Mobile IPv6 roaming in networks other than the home domain. The Internet draft identifies information that typically needs to be exchanged between a MN and an AAA Client in the network and suggests use of the new Diameter application in exchanges of this information between AAA Client and AAAv, between AAAv and AAAh, and between HA and the AAA infrastructure. However, no particular mechanism to convey information between the mobile node and the AAA Client is specified. This, together with other shortcomings, makes this solution unsatisfactory and non-complete.

Thus, the need for an appropriate mechanism for MIPv6 AAA remains.

SUMMARY

An object of the invention is to achieve a complete mechanism for combining terminal mobility and user authentication in networks with mobile nodes. Another object is to enable MIPv6 AAA.

This is achieved by means of a new EAP authentication protocol referred to as "EAP/MIPv6" (or "MIPv6 authentication method"). Preferably, the invention enables MIPv6 AAA by using a combination of PANA and Diameter as carrier protocols. The EAP/MIPv6 protocol can carry information that facilitates MIPv6 authentication, as well as dynamic MN home address allocation, dynamic HA allocation, distribution of security keys between HA and MN, and distribution of security keys between PAC and PAA for PANA security.

PANA is preferably used in carrying EAP/MIPv6 between MN/PAC and PAA/AAA Client. There are alternative carrier protocols, though. Diameter EAP Application [3] is generally used to transport EAP/MIPv6 between PAA/AAA Client and AAAv, and between AAAv and AAAh. The Diameter protocol is also used by AAAh for assignment to PAA/EP of security keys for PANA security, optional MIP packet filters via MIP filter rules, and optional QoS parameters etc. However, there may be embodiments using another suitable AAA protocol, such as Radius, instead of Diameter.

The exchanges between HA and the AAA infrastructure may for instance follow the AAAh-HA interface protocol specified in Diameter MIPv4 Application [2], or alternatively employ a mechanism similar to that currently used in 3GPP2 (i.e. [9]) in conjunction with the IKE [8] framework.

MIPv6 handoffs use a subset of the procedures used for MIPv6 initiation. For the handoff case, EAP/MIPv6 would only need to carry information that facilitates MIPv6 authentication, and distribution of security keys between PAC and PAA for PANA security.

For the case where EAP is used for WLAN authentication, e.g., EAP/AKA, PANA can be used for transporting EAP/AKA between PAC and PAA for WLAN access authentication

instead of [10]. By carrying multiple EAP sequences in a single PANA sequence, both EAP/AKA authentication of WLAN and EAP/MIPv6 can take place within a single PANA sequence for optimization purpose.

According to the authentication method of the invention, new EAP TLVs are defined for carrying MIPv6 authentication information. In case MD5 challenge authentication is used, these typically includes a MD5 Challenge attribute and a MD5 Response EAP-TLV attribute.

The authentication protocol preferably defines a number of additional EAP TLVs for dynamic MN home address allocation, dynamic HA allocation and distribution of security keys between HA and MN. These attributes are optional and there may be implementations lacking some or all of them. Furthermore, for distribution of security keys between PAC and PAA for PANA security, a PAC-PAA Pre-shared Key Generation Nonce EAP-TLV attribute is generally needed.

By means of the attributes like these, the EAP protocol is allowed to carry MIPv6-related auxiliary information, such as requests for dynamic MN home address allocation, dynamic Home Agent allocation, as well as nonces/seeds for creation of necessary security keys, in addition to the main IPv6 authentication information. This is a major advantage of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention may best be understood by reference to the following description and the accompanying drawing, in which:

Fig. 1 is a schematic view of a communication system for MIPv6 AAA in which the present invention may be used;

Fig. 2 is a signal flow diagram of MIPv6 initiation in accordance with a first exemplary embodiment of the present invention;

Fig. 3 is a signal flow diagram of MIPv6 initiation in accordance with a second exemplary embodiment of the present invention; and

Fig. 4 is a signal flow diagram of MIPv6 handoff in accordance with an exemplary embodiment of the present invention.

DETAILED DESCRIPTION

Introductory discussion

As mentioned in the background section, a proposal which attempts to specify a new application to Diameter that enables Mobile IPv6 roaming in networks other than its home has been raised in IETF [4]. It identifies the following information that typically needs to be exchanged between a MN and an AAA Client in the network: MIP Feature Data, EAP Data, Security Key Data, and Embedded Data. It also specifies the use of the new Diameter application in exchanges of the above information between AAA Client and AAAv, between AAAv and AAAh, and between HA and the AAA infrastructure.

Although [4] does not specify any particular mechanism to convey information between the mobile node and the AAA Client, the possibility to use the protocol defined by the IETF PANA WG has been mentioned. On the other hand, the PANA WG has recently identified EAP [6] as the payload for the PANA protocol and carrier for authentication methods [1]. In other words, PANA will carry EAP, which can carry various authentication methods. By the virtue of enabling transport of EAP above IP, any authentication method that can be carried as an EAP method is made available to PANA and hence to any link-layer technology. The PANA WG has assumed a clear division of labor between PANA, EAP and EAP methods. Defining new authentication methods, or deriving/distributing keys is considered outside the scope of PANA. Providing a secure channel that protects EAP and EAP methods against eavesdropping and spoofing is also not an objective of the PANA design.

This implies that apart from carrying the EAP, the PANA protocol will not be able to transport the other MIPv6-related auxiliary information such as MIP Feature Data, Security Key Data, and Embedded Data. Thus, there is no satisfactory prior-art mechanism for MIPv6 roaming in foreign networks and conveying necessary information between MN and AAA Client.

Another drawback of the solution in [4] is that it requires the AAA Client (and AAAv) to understand the authentication method and be aware of the contents of the exchanges (MIP Feature Data, EAP Data, Security Key Data, and Embedded Data) between the MN and the AAAh. It will not be possible to let the AAA Client act as mere pass-through agent, which is one of the major advantages of using EAP (and one of the assumptions for using PANA). Neither will it be possible to apply prior encryption between MN and AAAh (e.g., EAP/TTLS [5]) and the exchanges will be visible over the air interface. Security against eavesdropping, man-in-the-middle and other attacks is likely to be compromised.

These drawbacks and others are overcome by the present invention, according to which an EAP authentication protocol is proposed for combining the terminal mobility of MIPv6 with the user authentication of AAA in a most advantageous way, achieving a complete MIPv6 AAA solution.

Main principles as well as implementation details of the invention will now be described by way of example. General reference is made to the MIPv6 AAA actors and architecture illustrated in Fig. 1.

MIPv6 AAA using PANA and Diameter Combination

A new EAP authentication protocol "EAP/MIPv6" is defined to carry a "MIPv6 authentication method". EAP/MIPv6 should enable negotiation/enforcement of MIPv6 authentication (main goal), as well as support some auxiliary information that facilitate e.g., dynamic MN home address allocation, dynamic HA allocation, distribution of security keys between HA and MN, and distribution of security keys between PAC and PAA for PANA security. PANA is preferably used in carrying EAP/MIPv6 between MN/PAC and PAA/AAA Client. Alternatively, carrier protocols which satisfy EAP requirements on lower layer ordering guarantees as in PPP and [10] may be used to carry EAP/MIPv6 between the MN and AAA Client. Specifically for the 3GPP2 CDMA2000 case, it is possible to carry EAP/MIPv6 between the MN and AAA Client using PPP Data Link Layer protocol encapsulation with protocol field value set to C227 (Hex) for EAP [6].

A preferred embodiment uses Diameter for communication between the AAA client and home server. Beyond the PAA/AAA Client towards and within the AAA infrastructure, Diameter

EAP Application [3] is then used to encapsulate EAP/MIPv6 within Diameter, that is, EAP/MIPv6 is carried between the PAA/AAAClient and AAAh. The Diameter protocol is used by AAAh for optional assignment of MIP packet filters via MIP filter rules to the PAA/EP and HA, which correspond to the filter enforcement points. The Diameter protocol is also used by AAAh for distribution of security keys to PAA for PANA security, and optional signaling of QoS parameters etc.

It should be noted that even though Diameter is the preferred choice, it may sometimes be appropriate to instead use another AAA protocol, such as Radius, with modifications obvious to the man skilled in the art.

Regarding the communication between HA and the AAA infrastructure for exchange of security keys (necessary to establish SA between HA and MN) and accounting, two possibilities are suggested. One possibility is to employ the AAAh-HA interface protocol specified in Diameter MIPv4 Application [2]. Another possibility is to employ a mechanism similar to that currently used in 3GPP2 (i.e. [9]) in conjunction with the IKE [8] framework, to distribute dynamic pre-shared keys between MN and HA. A KeyID is used by the HA to retrieve (or generate) the HA-MN pre-shared key from the AAAh (exactly how this is done is vendor/operator implementation specific, and out of scope of this patent disclosure). The KeyID is generated by the AAAh and upon successful authentication sent to the MN, which in turn sends it to the HA using IKE.

MIPv6 handoffs use a subset of the MIPv6 initiation procedures described above. For the handoff case, since the MN has already been previously assigned a home address and a HA prior to handoff, EAP/MIPv6 would only need to carry information that facilitate MIPv6 authentication, and distribution of security keys between PAC and PAA for PANA security. The MIPv6 authentication which takes place is for authentication to use the newly acquired CoA. As with the MIPv6 initiation case, Diameter protocol is used by AAAh for assignment to PAA/EP of optional MIP packet filters via some kind of MIP filter rule, security keys for PANA security, and optional QoS parameters etc.

When both EAP/AKA for WLAN access authentication, and EAP/MIPv6 have to be carried out, it is proposed to allow single traversal to carry out both simultaneously to save time and

facilitate fast handoff (both AAAv and AAAh are traversed). PANA is used in carrying EAP/MIPv6 between PAC and PAA/AAA Client. PANA can also used for transporting EAP/AKA between PAC and PAA for WLAN access authentication instead of [10]. By carrying multiple EAP sequences in a single PANA sequence, both EAP/AKA for WLAN authentication and EAP/MIPv6 can take place within a single PANA sequence for optimization purposes.

New EAP attributes and exemplary signal flows

In this section, implementation features of the proposed authentication protocol according to the invention will be described. Examples of EAP/MIPv6 protocol details are provided to show the overall flow and viability of concept.

The authentication method of the invention involves new EAP TLVs carrying information that facilitates MIPv6 authentication, dynamic MN home address allocation, dynamic HA allocation, distribution of security keys between HA and MN, and distribution of security keys between PAC and PAA for PANA security.

The following new EAP TLVs are preferably defined under EAP/MIPv6:

i) *MD5 Challenge EAP-TLV attribute*
ii) *MD5 Response EAP-TLV attribute*
iii) *MIPv6 Home Address Request EAP-TLV attribute*
iv) *MIPv6 Home Address Response EAP-TLV attribute*
v) *MIPv6 Home Agent Address Request EAP-TLV attribute*
vi) *MIPv6 Home Agent Address Response EAP-TLV attribute*
vii) *HA-MN Pre-shared Key Generation Nonce EAP-TLV attribute*
viii) *IKE KeyID EAP-TLV attribute*
ix) *HA-MN IPSec SPI EAP-TLV attribute*
x) *HA-MN IPSec Key Lifetime EAP-TLV attribute*
xi) *PAC-PAA Pre-shared Key Generation Nonce EAP-TLV attribute*

By means of (some or all of) these attributes, the EAP protocol can, in addition to the main IPv6 authentication information, carry MIPv6-related auxiliary information, which is a considerable advantage. The MIPv6-related auxiliary information can e.g. comprise requests

for dynamic MN home address allocation, dynamic Home Agent allocation, as well as nonces/seeds for creation of necessary security keys.

Different authentication protocols are possible for EAP/MIPv6. A preferred embodiment of the invention proposes implementation through MD5-Challenge authentication, but other protocols also lie within the scope of the invention. The following EAP-TLV attributes are defined for MIPv6 authentication:

i) MD5 Challenge EAP-TLV attribute

This represents the octet string generated randomly by the AAAh and sent to MN for MD5 challenge.

ii) MD5 Response EAP-TLV attribute

This represents the octet string generated as a result of MD5 hash function with the shared secret key between AAAh and MN.

The following EAP-TLV attributes are preferably defined for dynamic MN home address allocation:

iii) MIPv6 Home Address Request EAP-TLV attribute

This represents a request for a dynamically allocated MIPv6 home address for the authenticated MN. It will be requested by the MN to the AAAh when the MN initially requests to be authenticated and given MIPv6 service. This attribute is optional when the MN already has a previously assigned home address, e.g., during MIPv6 handoffs.

iv) MIPv6 Home Address Response EAP-TLV attribute

This represents a dynamic allocated MIPv6 home address for the authenticated MN. It will be notified to the MN from AAAh when the MN, which has requested for one, has been successfully authenticated. This attribute is optional when the MN already has a previously assigned home address, e.g., during MIPv6 handoffs.

The following EAP-TLV attributes are preferably defined for dynamic HA allocation:

v) MIPv6 Home Agent Address Request EAP-TLV attribute

This represents a request for an address of a dynamically allocated HA for the MN when successfully authenticated. It will be requested by the MN to the AAAh when a MN initially requests to be authenticated and given MIPv6 service. As the MIPv6 protocol has a dynamic HA discovery method to allocate the HA, this attribute is optional. This is also the case when the MN already has a previously assigned HA, e.g., during MIPv6 handoffs.

vi) MIPv6 Home Agent Address Response EAP-TLV attribute

This represents an address of a dynamic allocated HA for the authenticated MN. It will be notificd to the MN from the AAAh when a MN initially requests to be authenticated and given MIPv6 service. As the MIPv6 protocol has a dynamic home agent discovery method to allocate the home agent, this attribute is optional. This is also the case when the MN already has a previously assigned HA, e.g., during MIPv6 handoffs.

The following EAP-TLV attributes are preferably defined for distribution of security keys between HA and MN:

vii) HA-MN Pre-shared Key Generation Nonce EAP-TLV attribute

This represents the octet string generated randomly by MN as a seed for generating the pre-shared key between HA-MN. The MN can internally generate the HA-MN pre-shared key by using an appropriate hash algorithm on the combination of this nonce and the shared key between MN and AAAh. This attribute is optional when a valid HA-MN pre-shared key already exists, e.g., during MIPv6 handoffs.

viii) IKE KeyID EAP-TLV attribute

This represents the ID payload defined in [7]. The KeyID is generated by the AAAh and sent to the MN upon successful authentication. The KeyID includes some octets which informs the HA how to retrievc (or generatc) the HA-MN pre-shared key from AAAh. This attribute is optional, and would generally not be needed when the MN did not submit a HA-MN pre-shared key gencration nonce, i.e., a valid HA-MN prc-shared key already exists, e.g., during MIPv6 handoffs. It is also not needed for the case when the HA-MN pre-shared kcy is conveyed by the AAAh to the HA via the AAAh-HA interface defined in [2].

ix) HA-MN IPSec SPI EAP-TLV attribute

This represents the Security Parameter Index for IPSec between the HA and MN. This is generated by the HA and informed to the MN for the case when the HA-MN pre-shared key is conveyed by the AAAh to the HA via the AAAh-HA interface defined in [2]. This attribute is optional and is generally not needed when the MN did not submit a HA-MN pre-shared key generation nonce, i.e., a valid HA-MN pre-shared key already exists, e.g., during MIPv6 handoffs. It is also not needed for the case when the AAAh-HA interface defined in [2] is not used.

x) HA-MN IPSec Key Lifetime EAP-TLV attribute

This represents the Key Lifetime for IPSec between the HA and MN. This is generated by the HA and informed to the MN for the case when the HA-MN pre-shared key is conveyed by the AAAh to the HA via the AAAh-HA interface defined in [2]. This attribute is optional and is generally not needed when the MN did not submit a HA-MN pre-shared key generation nonce, i.e., a valid HA-MN pre-shared key already exists, e.g., during MIPv6 handoffs. It is also not needed for the case when the AAAh-HA interface defined in [2] is not used.

Finally, the following EAP-TLV attribute is preferably defined for distribution of security keys between PAC and PAA for PANA security:

xi) PAC-PAA Pre-shared Key Generation Nonce EAP-TLV attribute

This represents the octet string generated randomly by MN/PAC as a seed for generating the pre-shared key between PAC-PAA. The MN/PAC can internally generate the PAC-PAA pre-shared key by using an appropriate hash algorithm on the combination of this nonce and the shared key between MN and AAAh. This attribute is needed for PANA security.

Preferred schemes for handling MIPv6 initiation and handoff according to the invention are provided in the signaling flow diagrams Figs. 2, 3 and 4. The illustrated examples relate to MIPv6 AAA using a combination of PANA and Diameter as carrier protocols. The flow diagram in Fig. 2 illustrates MIPv6 initiation with use of an AAAh-HA interface according to [2] for exchange of a HA-MN pre-shared key. Another MIPv6 initiation scheme, illustrated in Fig. 3, uses IKE KeyID for exchange of a HA-MN pre-shared key. The signaling flows of Fig. 4 describe MIPv6 handoff in accordance with an examplary embodiment of the invention.

Concluding remarks/Benefits of the invention

A major advantage of the proposed EAP protocol is that it allows EAP to carry MIPv6-related auxiliary information in addition the main MIPv6 authentication information. This auxiliary information may include requests for dynamic MN home address allocation, dynamic Home Agent allocation, as well as nonces/seeds for creation of necessary security keys. The MIPv6-related auxiliary information are exchanged between the Mobile Node and AAAh (home AAA server), and there is no need for intermediaries like AAA Clients and AAAv (visited AAA servers) to understand the information.

Without the proposed solution, i.e. if EAP was not carrying the MIPv6-related auxiliary information, requirements would typically be placed on the carrier protocols like PANA and Diameter to carry this information. This leads to an increased complexity of the carrier protocols and to compromised security (as the information is also picked up by intermediaries AAA Clients and AAAv's).

To sum up, the invention achieves a complete MIPv6 AAA solution for the first time, and does not put unnecessary complexities on carrier protocols. It also enables security of information between the Mobile Node and home AAA server.

Although the invention has been described with reference to specific exemplary embodiments, it also covers equivalents to the described features, as well as modifications and variants obvious to a man skilled in the art.

REFERENCES

[1] Protocol for Carrying Authentication for Network Access (PANA), D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, A. Yegin, 2003-4-3

[2] Diameter Mobile IPv4 Application, P. Calhoun, T. Johansson, C. Perkins, 2003-4-29

[3] Diameter Extensible Authentication Protocol (EAP) Application, T. Hiller, G. Zorn, March 2003

[4] Diameter Mobile IPv6 Application, Stefano M. Faccin, Franck Le, Basavaraj Patil, Charles E. Perkins, April 2003

[5] EAP Tunneled TLS Authentication Protocol, Paul Funk, Simon Blake-Wilson, November 2002

[6] PPP Extensible Authentication Protocol (EAP), RFC2284, L. Blunk, J. Vollbrecht, March 1998

[7] Internet Security Association and Key Management Protocol (ISAKMP), RFC2408, D. Maughan, M. Schertler, M. Schneider, J. Turner, November 1998

[8] The Internet Key Exchange (IKE), RFC2409, D. Harkins, D. Carrel, November 1998

[9] 3GPP2 X.P0011 Ver.1.0-9, 3GPP2 Wireless IP Network Standard, February, 2003

[10] IEEE Standard 802.1X, Local and metropolitan area networks – Port-Based Network Access Control

ABBREVIATIONS

Table 1 below contains a list of abbreviations and acronyms used in this document.

Table 1

AAA - Authentication Authorisation and Accounting
AAAh - Home AAA
AAAv - Visited AAA
AKA - Authentication Key Agreement
EAP - Extensible Authentication Protocol
EP - Enforcement Point
HA - Home Agent
IKE - Internet Key Exchange
IPSec - IP Security
ISAKMP - Internet Security Association and Key Management Protoc
MD5 - Message Digest 5
MIPv6 - Mobile IP version 6
MN - Mobile Node
PAA - PANA Authentication Agent
PAC - PANA Client
PANA - Protocol for carrying Authentication for Network Access
SPI - Security Parameters Index
TLS - Transport Layer Security
TLV - Type Length Value
TTLS - Tunneled TLS
WLAN - Wireless Local Area Network

ABSTRACT

The present invention proposes an authentication method for mobile IP communication, which enables MIPv6 AAA, for example through a combination of PANA and Diameter as carrier protocols. A new EAP authentication protocol is provided that can carry information facilitating MIPv6 authentication, dynamic MN home address allocation, dynamic HA allocation, distribution of security keys between HA and MN, and distribution of security keys between PAC and PAA for PANA security. The protocol preferably defines a number of new TLV attributes for carrying this kind of information.

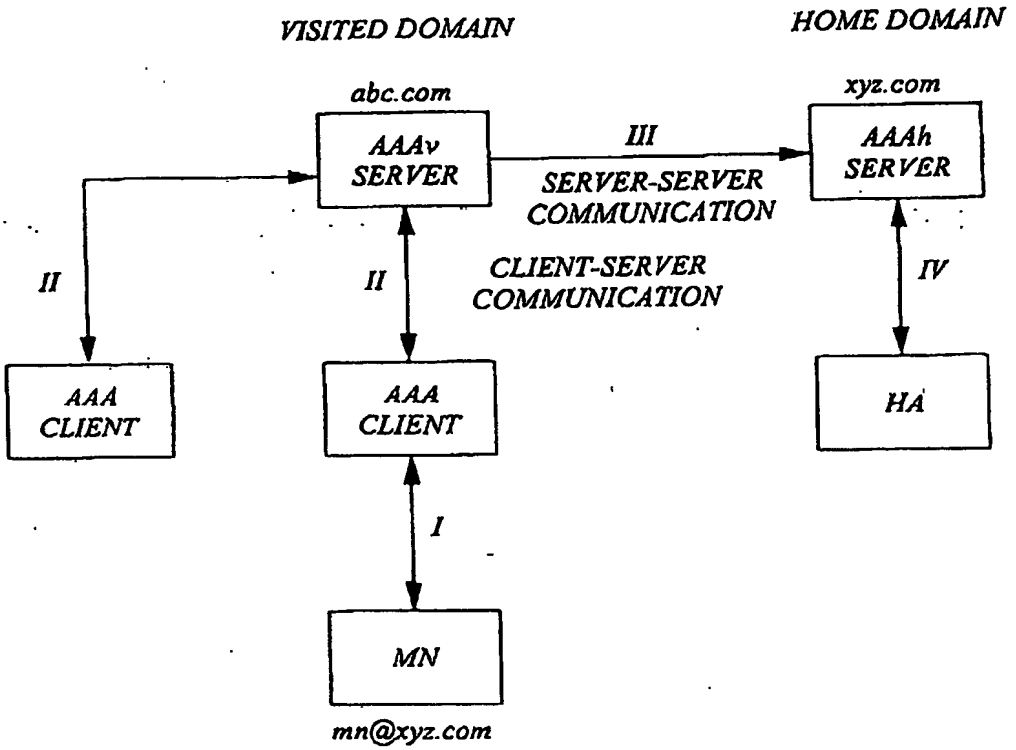
VISITED DOMAIN
HOME DOMAIN
abc.com
xyz.com
AAAv SERVER
III
AAAh SERVER
SERVER-SERVER COMMUNICATION
II
II
CLIENT-SERVER COMMUNICATION
IV
AAA CLIENT
AAA CLIENT
HA
I
MN
mn@xyz.com

FIG. 1

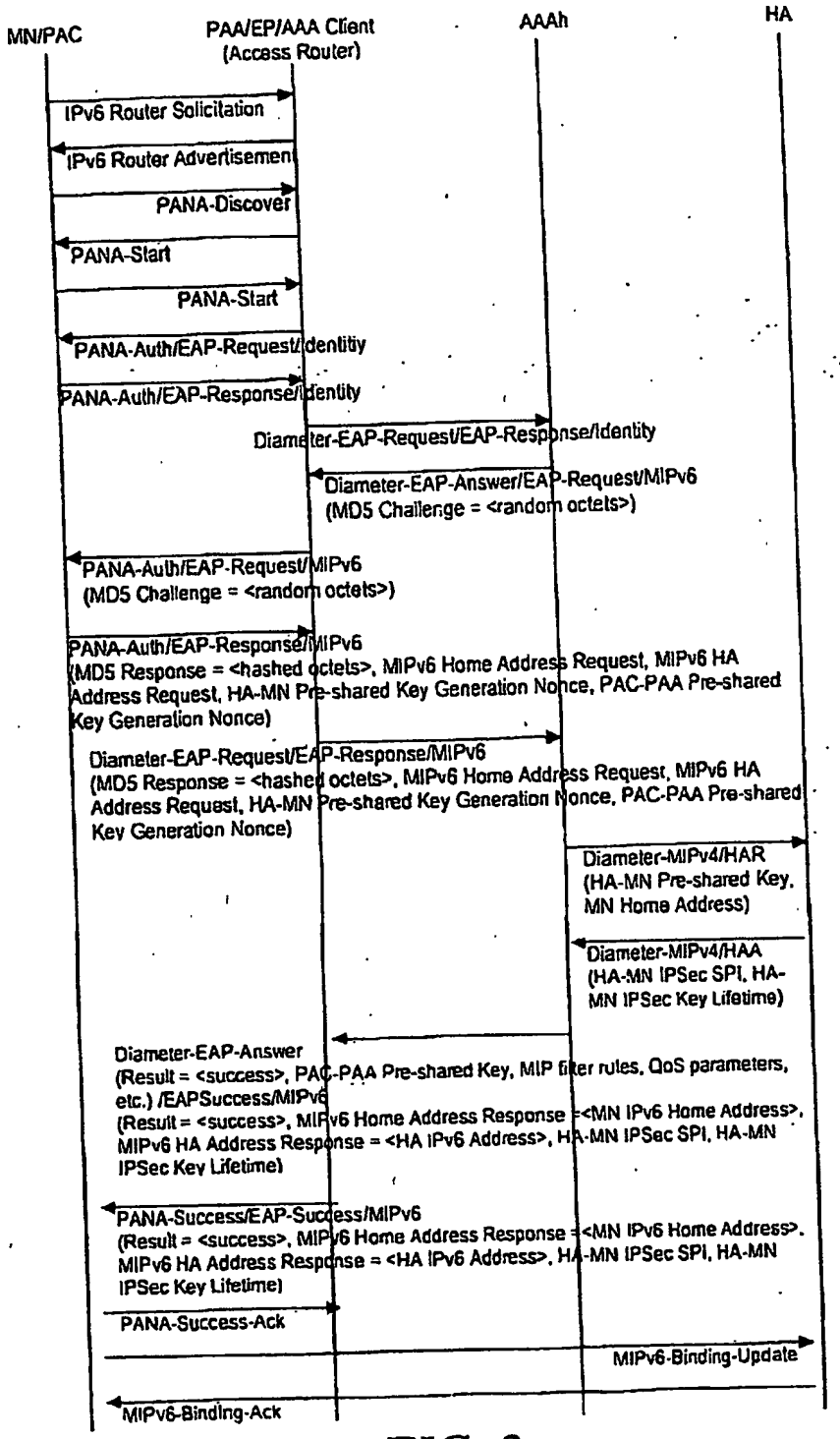
MN/PAC
PAA/EP/AAA Client (Access Router)
AAAh
HA
IPv6 Router Solicitation
IPv6 Router Advertisement
PANA-Discover
PANA-Start
PANA-Start
PANA-Auth/EAP-Request/Identity
PANA-Auth/EAP-Response/Identity
Diameter-EAP-Request/EAP-Response/Identity
Diameter-EAP-Answer/EAP-Request/MIPv6 (MD5 Challenge = <random octets>)
PANA-Auth/EAP-Request/MIPv6 (MD5 Challenge = <random octets>)
PANA-Auth/EAP-Response/MIPv6 (MD5 Response = <hashed octets>, MIPv6 Home Address Request, MIPv6 HA Address Request, HA-MN Pre-shared Key Generation Nonce, PAC-PAA Pre-shared Key Generation Nonce)
Diameter-EAP-Request/EAP-Response/MIPv6 (MD5 Response = <hashed octets>, MIPv6 Home Address Request, MIPv6 HA Address Request, HA-MN Pre-shared Key Generation Nonce, PAC-PAA Pre-shared Key Generation Nonce)
Diameter-MIPv4/HAR (HA-MN Pre-shared Key, MN Home Address)
Diameter-MIPv4/HAA (HA-MN IPSec SPI, HA-MN IPSec Key Lifetime)
Diameter-EAP-Answer (Result = <success>, PAC-PAA Pre-shared Key, MIP filter rules, QoS parameters, etc.) /EAPSuccess/MIPv6 (Result = <success>, MIPv6 Home Address Response = <MN IPv6 Home Address>, MIPv6 HA Address Response = <HA IPv6 Address>, HA-MN IPSec SPI, HA-MN IPSec Key Lifetime)
PANA-Success/EAP-Success/MIPv6 (Result = <success>, MIPv6 Home Address Response = <MN IPv6 Home Address>, MIPv6 HA Address Response = <HA IPv6 Address>, HA-MN IPSec SPI, HA-MN IPSec Key Lifetime)
PANA-Success-Ack
MIPv6-Binding-Update
MIPv6-Binding-Ack

FIG. 2

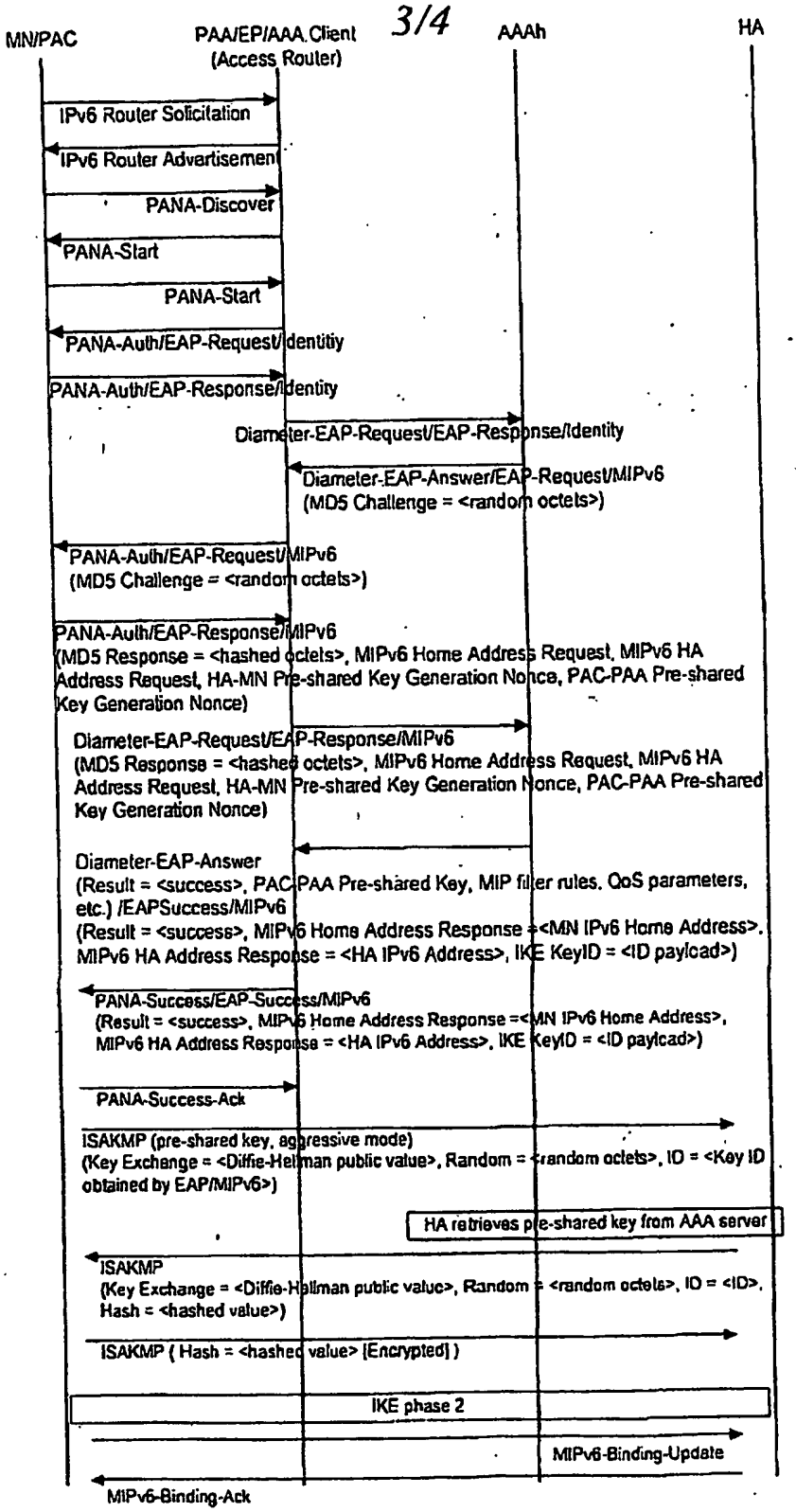
MN/PAC
PAA/EP/AAA Client (Access Router)
AAAh
HA
IPv6 Router Solicitation
IPv6 Router Advertisemen
PANA-Discover
PANA-Start
PANA-Start
PANA-Auth/EAP-Request/Identitiy
PANA-Auth/EAP-Response/Identity
Diameter-EAP-Request/EAP-Response/Identity
Diameter-EAP-Answer/EAP-Request/MIPv6 (MD5 Challenge = <random octets>)
PANA-Auth/EAP-Request/MIPv6 (MD5 Challenge = <random octets>)
PANA-Auth/EAP-Response/MIPv6 (MD5 Response = <hashed octets>, MIPv6 Home Address Request, MIPv6 HA Address Request, HA-MN Pre-shared Key Generation Nonce, PAC-PAA Pre-shared Key Generation Nonce)
Diameter-EAP-Request/EAP-Response/MIPv6 (MD5 Response = <hashed octets>, MIPv6 Home Address Request, MIPv6 HA Address Request, HA-MN Pre-shared Key Generation Nonce, PAC-PAA Pre-shared Key Generation Nonce)
Diameter-EAP-Answer (Result = <success>, PAC-PAA Pre-shared Key, MIP filter rules, QoS parameters, etc.) /EAPSuccess/MIPv6 (Result = <success>, MIPv6 Home Address Response =<MN IPv6 Home Address>, MIPv6 HA Address Response = <HA IPv6 Address>, IKE KeyID = <ID payload>)
PANA-Success/EAP-Success/MIPv6 (Result = <success>, MIPv6 Home Address Response =<MN IPv6 Home Address>, MIPv6 HA Address Response = <HA IPv6 Address>, IKE KeyID = <ID payload>)
PANA-Success-Ack
ISAKMP (pre-shared key, aggressive mode) (Key Exchange = <Diffie-Hellman public value>, Random = <random octets>, ID = <Key ID obtained by EAP/MIPv6>)
HA retrieves pre-shared key from AAA server
ISAKMP (Key Exchange = <Diffie-Hellman public value>, Random = <random octets>, ID = <ID>, Hash = <hashed value>)
ISAKMP (Hash = <hashed value> [Encrypted])
IKE phase 2
MIPv6-Binding-Update
MIPv6-Binding-Ack

FIG. 3

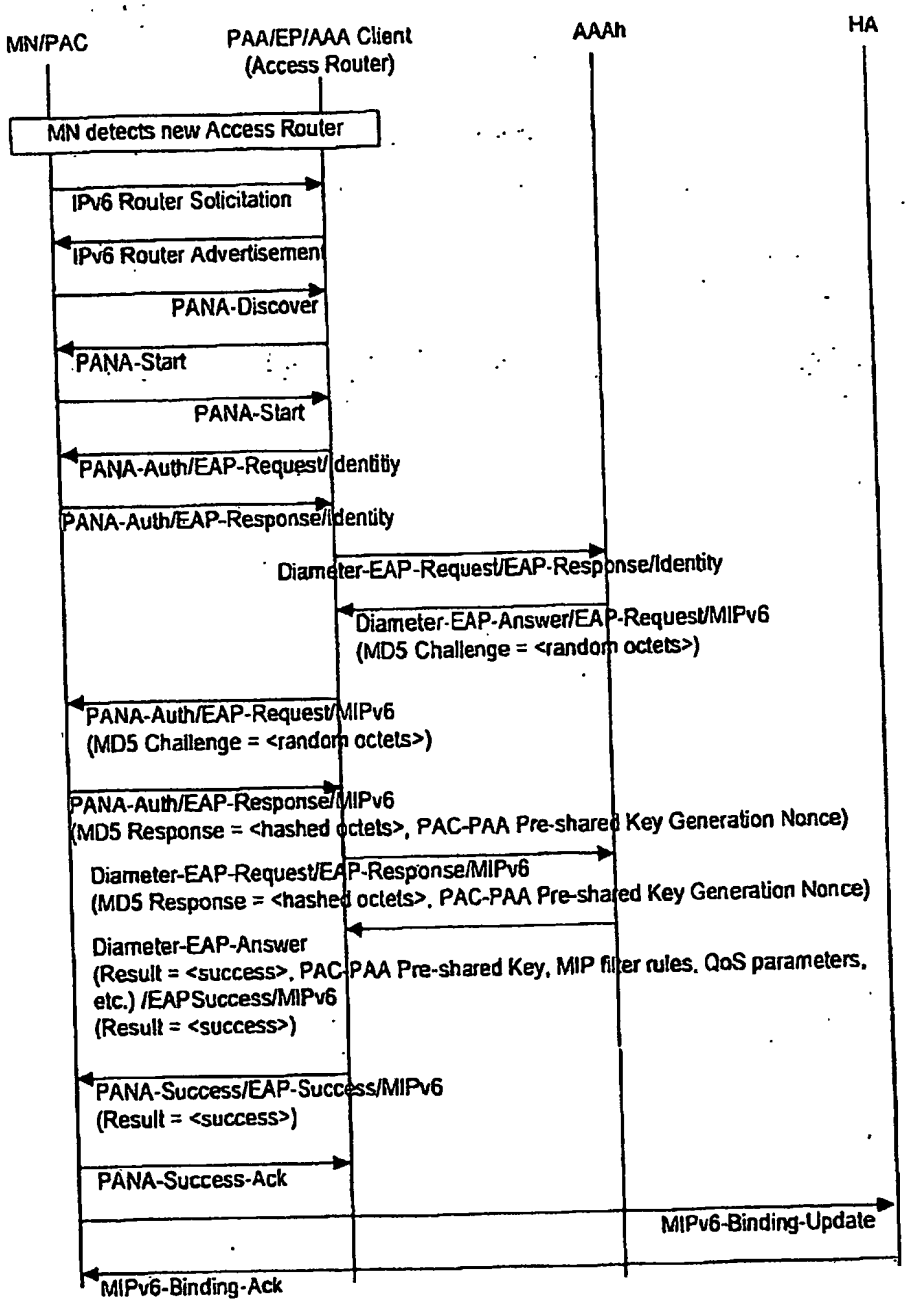
MN/PAC
PAA/EP/AAA Client
(Access Router)
AAAh
HA
MN detects new Access Router
IPv6 Router Solicitation
IPv6 Router Advertisement
PANA-Discover
PANA-Start
PANA-Start
PANA-Auth/EAP-Request/Identity
PANA-Auth/EAP-Response/Identity
Diameter-EAP-Request/EAP-Response/Identity
Diameter-EAP-Answer/EAP-Request/MIPv6
(MD5 Challenge = <random octets>)
PANA-Auth/EAP-Request/MIPv6
(MD5 Challenge = <random octets>)
PANA-Auth/EAP-Response/MIPv6
(MD5 Response = <hashed octets>, PAC-PAA Pre-shared Key Generation Nonce)
Diameter-EAP-Request/EAP-Response/MIPv6
(MD5 Response = <hashed octets>, PAC-PAA Pre-shared Key Generation Nonce)
Diameter-EAP-Answer
(Result = <success>, PAC-PAA Pre-shared Key, MIP filter rules, QoS parameters,
etc.) /EAPSuccess/MIPv6
(Result = <success>)
PANA-Success/EAP-Success/MIPv6
(Result = <success>)
PANA-Success-Ack
MIPv6-Binding-Update
MIPv6-Binding-Ack

FIG. 4